华御 Cross 下一代防火墙

产品技术白皮书

北京华御科技有限公司

2016 年 9 月

目　录

第1部分 概述

根据 Verizon 发布的《2014 年数据泄漏调查报告》显示，企业需要花费数月或更长时间才能发现 66% 的安全违规事件。对于受经济利益驱使的攻击，客户、合作伙伴、执法部门或其他外部机构发现了其中的 91%。

一次窃取信用卡数据、公司机密或其他敏感信息的攻击会造成严重损失。据 Ponemon Institute 发布的《2014 年数据泄露成本调查报告》显示，2013 年企业数据泄漏的平均成本为 350 万美元，比上一年增加了 15%。据估算，2014 年 Target 公司数据泄漏的损失至少达 1.48 亿美元。

此类引人瞩目的数据泄漏事件的稳步增加引起了人们的深切担忧。有观点认为，“世界上只有两类机构：一类是已遭受黑客攻击的机构，另一类是不知道自己曾遭受黑客攻击的机构”。对此，美国司法部长 Eric Holder、前美国国家安全、基础设施保护和反恐协调官 Richard Clarke 以及联邦调查局局长 James Comey 都表示认同。从政府机构、全球银行业巨头、大型零售商乃至最具安全意识的国防承包商等各类机构都曾深受其害。

在应用需求的不断推动下，网络技术得到了飞速发展；而网络技术的进步则又反过来推动应用的发展，应用与网络之间是相辅相成、相互促进的。随着万兆到核心/千兆到桌面、Web2.0、虚拟化、物联网、网络音频/视频、P2P、云计算等各种新应用、新业务层出不穷，传统的基于端口进行应用识别和访问控制的防火墙，已远远无法满足各种新应用下安全防护的需求，故推出全新华御 Cross 下一代防火墙。

1.1 产品简介

华御 Cross 下一代防火墙是面向应用层设计，能够精确识别用户、应用和内容，具备完

整安全防护能力，能够全面替代传统防火墙，并具有强劲应用层处理能力的全新网络安全设备，华御 Cross 下一代防火墙解决了传统安全设备在应用管控、应用可视化、应用内容防护等方面的巨大不足，同时开启所有功能后性能不会大幅下降。

华御 Cross 下一代防火墙不但可以提供基础网络安全功能 ,如状态监测、VPN、抗 DDos、NAT 等；还实现了统一的应用安全防护，可以针对一个入侵行为中的各种技术手段进行统一的检测和防护，如应用扫描、漏洞利用、WEB 入侵、非法访问、蠕虫病毒、带宽滥用、恶意代码等。华御 Cross 下一代防火墙可以为不同规模的行业用户的数据中心、广域网边界、互联网边界等场景提供更加精细、更加全面、更高性能的应用内容防护方案。

其核心理念是在用户网络边界建立以应用为核心的网络安全策略 ,通过逐层递进方式实现用户/应用行为的可视、可控、合规和安全，最终保障网络应用被安全高效的使用。

更精细的应用层安全控制：

1、贴近国内应用、持续更新的应用识别规则库

2、支持包括 AD 域、Radius 等多种用户身份识别方式

3、面向用户与应用策略配置，减少错误配置的风险

更全面的内容级安全防护：

1、基于攻击过程的服务器保护，防御黑客扫描、入侵、破坏三步曲

2、强化的 WEB 应用安全，支持多种 SQL 注入防范、XSS 攻击、CSRF、权限控制等

3、完整的终端安全保护，支持漏洞、病毒防护等

4、双向内容检测，功能防御策略智能联动

1.2 互联网给网络管理带来的挑战

随着信息技术的飞速发展和广泛应用，网络已经渗透到社会的各个领域，成为人们工作、学习、生活中不可或缺的一部分。互联网的商业和通讯业务也随之得到快速增长，在为组织带来更多商业机会、提升组织生产效率的同时，相应地也降低了组织运营、生产和沟通成本。目前，不论政府、学校、企事业单位或是个人与网络的联系越来越紧密，网络一旦出现故障，将严重影响到工作、学习、生活。但是这些年网络安全安全事故层出不穷，安全风险比以往更加难以察觉，对社会各行各业都产生严重的影响。

1.3 应用网络时代，网络面临的问题

随着 WEB 2.0 为代表的下一代网络技术的迅猛发展，WEB 化应用呈现出爆发式的增长趋势，基于互联网的应用从最初的文件共享、文件传输（FTP）、静态网页浏览（HTML）以及 Telnet 等内容单一、静态的、简单、小规模的应用，逐步发展为包括 E-Mail、ERP、OA、CRM、新闻信息、文件共享、视频会议、VoIP、即时通讯、网络游戏、电子商务、电子政务以及移动终端应用等等在内的动态的、大规模的、复杂的应用。网络承载的内容日益丰富，变得更加复杂、多样化。当今，互联网进入了应用级网络时代，逐步成为一个虚拟的真实社会。P2P 传输、网络电视、网络游戏、在线聊天、Web 视频、股票软件、网上银行、数据库、物流供应链、各种论坛以及大量未知的内容和信息纷纷涌进网络。

传统的网络安全设备，如防火墙、入侵检测系统、防病毒软件、反垃圾邮件系统等，均已远远不能满足用户对自身网络的安全防护诉求。具体表现如下：

- **基于端口的访问控制已失效**

传统防火墙只能对网络流量进行基于端口的协议识别。而下一代网络中的大量应用可以直接复用同一标准协议的知名端口（如 80 端口已不再专属 HTTP，可被 P2P 使用）进

行传输，或者直接承载在标准协议中（如 Web 视频直接承载在 HTTP 协议中）。因此，传统防火墙仅基于端口的控制方式已无法实现精确管控，比如，允许访问 80 端口的策略很可能会让不期望的非法流量（如 P2P）通过，甚至让黑客程序借此漏洞发动网络攻击，若完全禁止 80 端口则会殃及 Web 应用，导致正常的网页访问无法进行。

同样，流量控制和管理也到了细分应用种类的地步，传统的基于端口的粗放型流量管理不仅可能会“误伤”应该保证的良性应用，更可能会“助长”不良应用。

- **基于 IP 地址的访问控制已不可靠**

传统防火墙通过 IP 地址对各安全区域进行访问控制，同时对威胁和应用来源进行跟踪审计。然而，除了固定的 IP 接入方案，随着无线通信和移动计算设备的飞速发展，越来越多的企业给员工配置移动办公设备，甚至允许员工自带私有设备工作。在这种多网多终端接入的环境下， IP 地址分配具有极强的随机性和不唯一性，IP 地址本身对用户身份信息的传递已经越来越不具有代表性。进而，传统的通过 IP 地址来进行用户访问控制已不再完全有效。而对网络访问者真正身份的全面有效、深度广泛的鉴定识别，才是适应社会和网络发展的最有效手段

- **入侵防御设备**

应用安全防护体系不完善，只能针对操作系统或者应用软件的底层漏洞进行防护，缺乏针对 Web 攻击威胁的防御能力，对 Web 攻击防护效果不佳。缺乏攻击事后防护机制，不具备数据的双向内容检测能力，对未知攻击产生的后果无能为力，如入侵防御设备无法应对来自于 web 网页上的 SQL，XSS 漏洞，无法防御来自内网的敏感信息泄露或者敏感文件过滤等等。

- **网络应用可见性差，存在法律风险**

一份来自于 IDC 的权威数据显示：80%以上的 IT 管理人员无法准确了解自己的网络。对网络管理来说，自己的网络就像一个黑盒子，里面都跑了些什么应用以及网络的状况根本不清楚，而管理员无法知道异常流量的类型、来源、具体流向、流量大小、持续的时间等，也无法有效规划网络资源的使用，导致网络管理处于无序状态。

为了加强对互联网的控制和管理，公安部颁发的 82 号令要求各机构要保存至少 3 个月的访问日志，以便协助公安调查取证。因此，如无有效的管理手段，企业内部对互联网资源的非法访问，比如访问色情、赌博、犯罪网站、发表反动言论、泄露重大机密等，都会触犯相关法律，给企业带来法律风险。

第2部分 产品优势技术

随着网络带宽的增加，网络应用以成倍的速度增加，应用层应用在无情地免费地侵蚀着宝贵的网络带宽，而网络安全的威胁更多的来源于应用层，对应用层的网络访问控制需要采用新的解决方案。精确的识别出应用、阻断有安全隐患的应用、保证合法应用正常使用、防止端口盗用等问题，已成为现阶段企事业用户对网络安全担忧的主题之一。

2.1 精细的应用层安全防护

华御 Cross 下一代防火墙采用 DPI 的识别方式使得应用层协议可视化可控，华御 Cross 下一代防火墙可以根据应用的行为和特征实现对应用进行识别和控制，而不仅仅依赖于端口或标准协议，摆脱了传统设备只能通过 IP 地址或者五元组控制的粗粒度，即使加密过的数据流也能进行管控。

目前，华御 Cross 下一代防火墙可以识别 700 多种应用，识别上千种网络行为动作，还可以与多种认证系统（AD、LDAP、Radius 等）无缝对接，自动识别出网络当中 IP 地址【MAC 地址、用户身份】对应的用户信息，并建立组织的用户分组结构；满足了普通互联网边界行为管控的要求。可以识别和控制丰富的内网应用，如迅雷 P2P、RDP、Lotus Notes、RTX、Citrix、Oracle EBS、金蝶 EAS、用友 NC、U8、SAP、LDAP 等，针对用户应用系统更新服务的诉求，华御 Cross 下一代防火墙还可以精细识别 Microsoft SHAREPOINT、奇虎 360、Symantec、 Sogou、Kaspersky、金山毒霸、江民杀毒等软件更新，保障在安全管控严格的环境下，系统软件更新服务畅通无阻。

因此，通过应用的协议识别制定的二到七层的应用访问控制策略，可以为用户提供更加精细和直观化控制界面，在一个界面下完成多套设备的运维工作，提升工作效率。

2.2 WEB 应用的安全防护

华御 Cross 下一代防火墙融合了漏洞防护、Web 安全防护等多种安全技术 ,具备 12000 多条漏洞特征库、木马插件等恶意内容特征库、800 多条 Web 应用威胁特征库，可以全面识别各种应用层和内容级别的各种安全威胁。提供 URL 过滤、文件过滤、ActiveX 过滤、脚本过滤等多种 WEB 安全防护手段通过对应用流中的数据报文内容进行探测，从而确定数据报文的真正应用。

WEB 应用防护通过主动防御已知和未知攻击，实时阻断各种黑客攻击，如 SQL 注入、XSS 攻击、网站扫描、WEB SHELL、会话劫持攻击等。

1. 防 SQL 注入攻击

SQL 注入攻击产生的原因是由于在开发 WEB 应用时，没有对用户输入的数据做合法性检查和判断，用户在提交一段数据库查询代码，根据程序返回的结果，获得默写他想得知的数据 ,这就是所谓的 SQL 注入。华御 Cross 下一代防火墙通过高效的 URL 过滤技术，过滤 SQL 注入的关键信息，从而有效的避免网站服务器受到的 SQL 注入攻击。

2. 防 XSS 跨脚本攻击

跨站攻击产生的原理是攻击者通过向 WEB 页面里插入恶意 HTML 代码，从而达到特殊目的。华御 Cross 下一代防火墙通过先进的数据包正则表达式匹配原理，可以准确地过滤数据包中包含的跨站式攻击的恶意代码，从而保护用户的 WEB 服务器安全。

2.3 应用层带宽管理

华御 Cross 下一代防火墙内置专业流量管理产品以应用对象设置、用户对象设置、时间对象设置、带宽通道对象设置、用户自定义对象设置基础，通过应用控制、流量管理、

内容过滤等策略，最大限度地满足用户在流量管理方面的不同需求，实现用户网络人性化的精确管理。专业流量管理产品满足了企业不同业务主次之分，系统分为 0-7 共 8 个 QoS 优先级控制策略，从而为指定的应用和通道提供差异化的影响级别。同时也可以为特定的实时应用，如视频会议、VOIP 等，预留固定的带宽，保证实时应用的流畅使用。

2.4 IPS 漏洞防护

支持 12000 多种流量异常特征库 ,并可以按优先级区分不同类型的漏洞攻击 ,按“高”，“中”，“低”区分；包括敏感信息泄露 DOS 攻击/尝试获取用户特权的攻击/尝试获取管理员特权的攻击/网络流量中发现可执行文件的注入/可疑关键字和可疑文件的注入/远程过程调用告警/网络木马程序注入/客户端使用可疑端口通信/可疑的网络扫描/篡改标准协议和非法事件的告警/潜在的 web 攻击/ICMP 告警/异常内容告警/公司机密泄露/尝试用默认账号窃取信息等。

2.5 网络病毒防护

病毒库数量：100,000+，定期更新，基于流引擎查毒技术，针对 HTTP、FTP、SMTP、POP3、IMAP 等协议进行查杀。

2.6 线速的状态检测防火墙

支持线路的带宽叠加，充分利用多条 Internet 接入；

支持多线路的策略路由，智能选择更快的线路接入 Internet；

支持三种工作模式（NAT 模式、透明桥模式、路由模式）;

支持状态检测防火墙（基于 IP/IP 段/IP 组、IP/MAC、PORT、时间控制等策略组合）;

支持关键字、文件类型、域名等内容过滤；

支持 VLAN 与静态路由；

第3部分 主要功能

3.1 识别与控制

3.1.1 用户身份识别

作为华御 Cross 下一代防火墙显著特征之一，华御 Cross 下一代防火墙对在线用户身份识别功能做了全面细致的支持。与传统的将用户认证策略混入防火墙策略配置中不同，华御 Cross 下一代防火墙将用户认证从防火墙复杂的策略配置中抽离出来，从逻辑上做出更合理清晰的呈现。

用户可对不同的安全区域指定不同的认证策略，并可根据不同场景选择不同的身份识别方案，例如，可从域控服务器直接获取身份信息，与第三方认证服务器（Radius、AD、LDAP）认证，本地帐号库认证，证书认证，以及结合以上多钟认证方式于一体的多因素认证。 同时，为方便用户理解和使用，华御 Cross 下一代防火墙对用户账号进行了集中管理和控制。只需集中配置好账户信息（包括 Radius、AD、LDAP、本地数据库、证书账号等）即可在用户认证策略、VPN 授权、设备管理员授权等多处便捷使用。

3.1.2 日志记录和统计报表

华御 Cross 下一代防火墙让用户随时可以了解当前网络正在发生什么。具体体现为，可实时了解当前网络中正遭受哪些威胁攻击（包括入侵攻击、病毒、恶意站点及敏感信息），以及相应的威胁等级、攻击数目等。

同时，用户可实时了解当前网络中一段时间以来各网络接口带宽使用情况，流量排名前十的应用以及流量使用排名前十的用户，并可实时互查应用与用户流量间的使用关系。除了实时网络状况，华御 Cross 下一代防火墙为用户提供按日、按周、按月、按年的安全

趋势分析报表以及以往所有的访问控制和安全日志。从而让用户对安全威胁、业务应用、用户流量、网络负载从时间、数量、程度上通过各种形象化图形和数据手段有了高度可视化的跟踪和了解。

3.2 应用层防护

3.2.1 入侵防护

华御 Cross 下一代防火墙内置 2500 多条威胁特征库，并将威胁入侵分为 5 大类，分别是按攻击手段分类（如获取 权限、信息收集类）、按技术手段分类（如蠕虫、P2P）、按流行程度分类（非常流行、中等流行）、按危险程度分类、按服务类型分类等（如 WWW、FTP 事件等）。华御 Cross 下一代防火墙可防护远程扫描、暴力破解、缓存区溢出、蠕虫病毒、木马后门、SQL 注入、跨站脚本等各种网络及应用攻击。同时支持用户自定义规则，建立规则组等功能，并能够对检测到的入侵事件实时告警、阻断、记录和提供统计报表。

3.2.2 URL 过滤

华御 Cross 下一代防火墙具有业界领先的基于云端的 URL 分类库，内含按照不同类型（如不良言论、色情暴力、网络“钓鱼”、论坛聊天等）划分的超过上亿条记录的 URL 信息，可实现对工作无关网站、不良信息、高风险网站的准确、高效过滤；

同时华御 Cross 下一代防火墙内置的 Web 信誉库，通过对互联网站点资源（域名、IP 地址、URL 等）进行威胁分析和信誉评级，将含有恶意代码的网站列入 Web 信誉库，可有效阻挡用户对挂马等不良信誉网站的有意或无意访问，实现对终端用户的安全保护。

3.2.3 防病毒

华御 Cross 下一代防火墙采用流模式和启发式文件扫描技术，对利用 HTTP、SMTP、

POP3、FTP、IM 等多种协议进行传播的病毒进行扫描，完成对木马病毒、蠕虫病毒、宏病毒、脚本病毒等的查杀，同时支持多线程并发控制、深层次压缩文件杀毒、病毒白名单等功能。

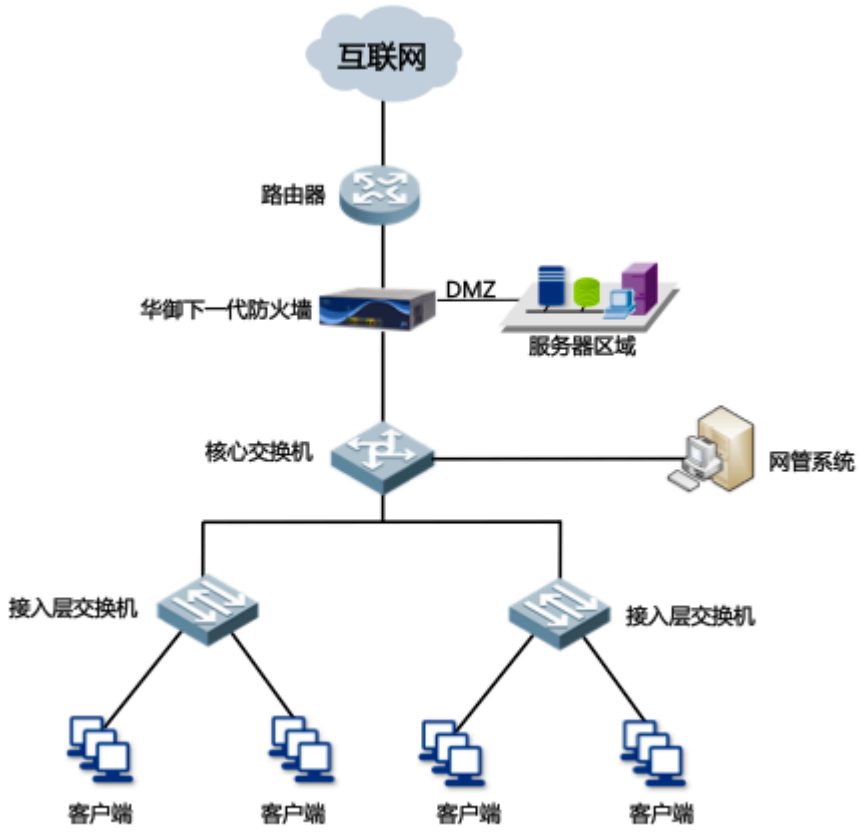
此外，华御 Cross 下一代防火墙将专业防病毒引擎和多核并行处理技术完美融合，实现高速病毒处理性能。

3.2.4 内容过滤

通过内容安全关键字，华御 Cross 下一代防火墙可对任意安全区域间交互的网页内容、搜索引擎信息内容、文件传输（文件名、格式、内容）、邮件收发（包括收发人、标题、内容、文件等）、论坛发言、服务器操作、以及即时通讯内容等进行基于内容关键字的准确检测、阻断、告警、记录和信息还原，实现深度内容安全管理与跟踪，避免用户机密信息、重要文件通过网络外泄，也避免了非法言论及不良信息的传播。

3.3 产品部署

防火墙通常部署在互联网的出口，如下图所示:



3.4 功能列表

部署模式	
网桥模式	支持以网桥模式部署，包括单桥和多桥的部署模式；支持 Bypass 功能。
路由模式	支持路由模式部署 ,可以作为出口网关 ,包括单出口和多出口的部署模式。
旁路模式	支持旁路模式部署。
混合模式	支持网桥和路由混合部署模式。
网管方式与网管策略	
WEB 管理	支持以 HTTP 及 SSL 加密的 WEB 图形化接口进行设备配置和管理，支持英语、简体中文、繁体中文接口。
SSH 管理	支持 SSH 命令行管理方式。
Console 管理	支持 Console 管理。
网管策略	管理权限分立：系统默认有超级管理员、审计管理员、只读管理员，可根据需要灵活定制管理员角色。 支持密码强度、口令尝试死锁、账户激活等安全管理功能。 通过网管策略，可允许部分 IP 能网管设备，以限制非法管理员访问设备。
网络功能	
静态路由	支持 IPv4、IPv6 静态路由功能。
OSPF 动态路由	支持 OSPF 动态路由。
RIP 动态路由	支持 RIP 动态路由。
策略路由	支持策略路由功能。

链路负载均衡	支持链路的负载均衡。
运营商路由选路	支持运营商路由选路。
持续路由	支持链路持续路由算法。
链路备份	支持主备链路的备份功能。
PPPOE 拨号	支持 PPPOE 拨号功能，支持多条 PPPOE 拨号做负载均衡。
DHCP 服务器	支持 DHCP 服务器功能。
DHCP 中继	支持 DHCP 中继功能。
DHCP 客户端	支持 IPv4、IPv6 DHCP 客户端功能。
DNS 代理	支持 DNS 代理功能。
DNS 缓存	设备作为 DNS 透明代理，缓存 DNS 记录。
动态 DNS 功能	支持动态 DNS 功能（花生壳）
VLAN	支持 VLAN 功能。
基础防火墙功能	
防火墙	支持基于状态监测的防火墙，不仅保障网关设备安全，还能保护组织内网安全。
NAT 转换	支持多对一的 PAT 转换、一对一的地址转换、端口映像等多种 NAT 转换策略。
VPN 功能	
PPTP VPN	支持 PPTP VPN。
IPSec VPN	支持标准的 IPSec VPN 功能。

L2TP VPN	支持 L2TP VPN
IPS 入侵防御	
防 dns 漏洞攻击	DNS 类规则识别各种 DNS 服务器漏洞，防止攻击者通过 DNS 服务器漏洞攻击用户。
防 mail 漏洞攻击	邮件库类规则识别各种邮件服务器漏洞，如 Sendmail、Foxmail、MS Exchange 等，防止攻击者通过邮件服务器漏洞攻击用户。
防 worm 漏洞攻击	蠕虫程序是一种可以自我复制的恶意程序，可以通过网络进行传播，消耗网络和系统资源。蠕虫规则识别蠕虫程序的传播，防止攻击者通过蠕虫程序破坏目标系统。
防 tftp 漏洞攻击	Tftp 类规则识别各种 tftp 服务器漏洞，如 3CDeamon、FutureSoft 等，防止攻击者通过 tftp 服务器漏洞攻击用户。
防 snmp 漏洞攻击	snmp 类规则识别各种 snmp 服务器漏洞，防止攻击者通过 snmp 服务器漏洞攻击用户。
防 ftp 漏洞攻击	Ftp 类规则识别各种 ftp 服务器漏洞，如 Serv-U、WU-FTPD、WS_FTP、3CDeamon 等，防止攻击者通过 ftp 服务器漏洞攻击用户。
防 shellcode 漏洞攻击	Shellcode 是一段小的程序，作为漏洞执行的负载，执行某种功能。Shellcode 规则识别 shellcode 代码 ,防止攻击者远程执行 shellcode 代码。
防 rpc 漏洞攻击	rpc 类规则识别各种 rpc 服务器漏洞，如 tooltalk、sadmind 等，防止攻击者通过 rpc 服务器漏洞攻击用户。
防 database 漏洞攻击	数据库类规则识别各种数据库服务器漏洞，如 Oracle、Sql server、Mysql 等，防止攻击者通过数据库服务器漏洞攻击用户。

防 web 漏洞攻击	Web 类规则识别各种 web 服务器漏洞，如 IIS、Apache 等，防止攻击者通过 web 服务器漏洞攻击用户。
防 system 漏洞攻击	系统类规则识别各种操作系统漏洞，如 Windows、Linux、Unix 等操作系统，防止攻击者通过操作系统漏洞攻击用户。
防 malware 漏洞攻击	Malware 就是植入你电脑中的恶意代码，它可以完全控制、破坏你的 PC、网络以及所有数据。malware 类规则识别各种 malware 程序，防止攻击者利用 malware 漏洞攻击用户。
防 trojan 漏洞攻击	木马软件是一种恶意软件，可以安装在用户计算机上，通过木马软件远程操控目标系统并执行各种操作。木马规则类识别木马软件的网络操作，防止攻击者通过木马软件控制目标系统。
防 telnet 漏洞攻击	Telnet 类规则识别各种 Telnet 服务器漏洞 ,防止攻击者通过 Telnet 服务器漏洞攻击用户。
防 botnet 漏洞攻击	botnet 类规则识别各种客户端 botnet 行为，防止攻击者通过 botnet 漏洞控制用户。
防 web_browse 漏洞攻击	Web 浏览器类规则识别各种 web 浏览器漏洞，如 IE、Firefox、Chrome 等，防止攻击者通过 web 浏览器漏洞攻击用户。
防 web_activex 漏洞攻击	ActiveX 是可以重用的软件组件程序，可以嵌入到 web 浏览器中使用。Web_activeX 类规则识别各种嵌入到浏览器的 ActiveX 控制漏洞，防止攻击者通过 ActiveX 控件漏洞攻击用户。
DOS/DDOS 防护	

DOS/DDOS 防护	支持 ARP 洪水攻击防护、IP 和端口扫描防护、 DOS/DDOS 防护(ICMP 洪水、UDP 洪水、SYN 洪水、DNS 洪水攻击防护)、未知协议类型防护、TearDrop 攻击防护、IP 数据块分片传输防护、LAND 攻击防护、WinNuke 攻击防护、Smurf 攻击防护、异常报文侦测防护等
服务器防护	
服务器防护	支持 Web 网站隐藏，包括 HTTP 响应报文头出错页面的过滤，web 响应报文头可自定义； 支持 FTP 服务应用信息隐藏包括：服务器信息、软件版本信息等； 支持 OWASP 定义 10 大 web 安全威胁，保护服务器免受基于 Web 应用的攻击，如 SQL 注入防护、XSS 攻击防护、CSRF 攻击防护、支持根据网站登录路径保护口令暴力破解；支持 web 站点扫描、web 站点结构扫描、漏洞扫描等扫描防护； 可严格控制上传文件类型，检查文件头的特征码防止有安全隐患的文件上传至服务器，并支持结合病毒防护、插件过滤等功能检查文件安全性； 支持指定 URL 的黑名单、加入排除 URL 目录，ftp 弱口令防护、telnet 弱口令防护等功能；
APT 检测	
APT 检测	内置强大的病毒、木马、间谍软件等恶意软件特征库，并且在不断的持续更新特征内容； 支持通过安全云实现虚拟沙盒动态检测异常行为。 支持云端基于白名单的终端安全检测，有效保护注册表、文件系统等，可

	实现快速统一的防护未知攻击；
僵尸网络告警	
僵尸网络告警	可基于行为特征判别可疑僵尸主机，支持 10 余种僵尸主机行为检测。
内容安全	
病毒防护	
病毒防护	基于流引擎查毒技术，支持对 HTTP、FTP、SMTP 和 POP3 协议流量查杀；能实时对 gzip，zip，rar 等压缩文件进行病毒查杀；云端特征库收录亿级病毒文件样本；检测到病毒后支持日志记录、阻断连接。
应用内容过滤	
海量 URL 库	预分类的海量 URL 地址库；支持手工添加新的 URL 地址和分类。
URL 过滤	支持 URL 过滤。
非标准端口 URL 管理	可以识别和管理部分论坛、网络聊天室等采用的非 TCP/80 端口的 URL 地址。
关键字过滤	对搜索引擎中输入的关键词、论坛微博发帖关键字、网页内容关键字、Telnet 关键字进行过滤，自动对搜索到的网址页面进行屏蔽，帮组企事业单位将涉及低俗的、非法的不良言论封堵掉。
HTTPS 网页识别	对于互联网上日益泛滥的加密网页进行识别和过滤，防止用户访问钓鱼网站、SSL 加密的色情、反动网站等以及加密邮件内容识别。
HTTP 文件传输过滤	可识别 HTTP 网页的文件上传和文件下载，并对文件的上传和下载进行过滤。
FTP 文件传输	可识别 FTP 网页的文件上传和文件下载，并对文件的上传和下载进行过

过滤	滤。
非标准端口 FTP 过滤	支持对非标准端口的 FTP 行为的识别；可过滤通过非标准端口的 FTP 进行文件的上传和下载。
邮件过滤	基于 WebMail 发件、SMTP 发件、POP3 收件，可根据发件人邮箱、关键字、附件类型、附件大小过滤。
终端类型	可针对移动终端、PC 及其他终端设定策略。
应用协议识别和控制	
常用协议	如 FTP、SMTP、TFTP、IMAP 等常用协议。
自定义协议	可自定义基于协议和端口的协议； 可根据协议、端口、报文长度、报文特征、目的 IP 等等信息自定义协议规则。
协议剥离	支持将特殊协议（如 MPLS、PPPoE、VLAN（Q-in-Q）、L2TP、GRE 等）的协议头剥离掉，这样可以对特殊协议封装内的原始数据进行认证、审计和控制。
HTTP 应用	网页文档下载、网页音频、HTTP 多线程下载、伪 IE 下载等多种方式的 HTTP 下载行为以及 QQ 空间应用、人人网、Facebook 等网页应用。
FTP 应用	FTP 上传文件、FTP 下载文件、FTP 命令。
视频网站浏览	凤凰视频、乐视网、优酷、土豆、搜狐视频、奇艺视频等网站的浏览。
WEB 视频	六间房、土豆、新浪视频、优酷视频、我乐网、酷六视频、搜狐视频等。
P2P 下载	电驴、迅雷、PP 点点通、酷狗、BT、网际快车、QQ 旋风、百度下吧、酷我八音盒等。

流媒体	PPLive、PPStream、蚂蚁电视、Qvod、风行网络电视、QQLive、UUsee 网络电视、皮皮影视（PPFilm）SopCast 等。
网络游戏	QQ 游戏、浩方对战平台、新浪游戏大厅、梦幻西游、问道、武林外传、泡泡堂、天龙八部、大话西游、征途、魔兽世界等。
即时通讯	QQ/TM、MSN、网易泡泡、淘宝旺旺、雅虎通、阿里旺旺、百度 HI、新浪 UC 等。
股票行情	同花顺、大智慧、东方财富通、和讯财经、安信行情、齐鲁证券等。
股票交易	同花顺、大智慧、安信行情、齐鲁证券、大福星、通达信等。
网上银行	中国银行、农业银行、建设银行、工商银行、招商银行等。
网络电话	Skype、ET263、YY 语音、Netmeeting 等。
网络存储	360 云盘、七牛云、新浪微云、腾讯微云、百度网盘、金山快盘等。
移动应用	移动终端的新闻资讯、社交通讯、购物支付、移动游戏、综合服务等分类。
网页邮箱	新浪邮箱、QQ 邮箱、163 邮箱、126 邮箱、搜狐邮箱等。
软件更新	诺顿、金山毒霸、趋势科技、网秦安全、熊猫卫士、360 安全卫士等。
远程控制	QQ 远程协助、SSH、Windows 远程桌面、VNC、teamview 等。
数据库	DB2、MySQL、Oracle、SQL 等。
自定义特征识别	可根据五元组，数据长度，数据报文特征字符串组合自定义特征。
流量控制	
流量优先级	可将应用流量划分为 高、中、低等共三个优先级，优先级越高的流量，优先传送。

最大带宽	为某些用户或特定应用指定最大带宽。
保障带宽	结合最大带宽和流量优先级 ,可为某些关键应用或者 VIP 客户保障一定带宽。
预留带宽	为某种特定应用或某些重点客户预留一定带宽，以保证在任何时间段、任何的网络使用环境中，某种流量都能得到预留的带宽。预留带宽不能被其他流量使用。
基于线路的流控	可以根据线路进行流量管理。
基于应用的流控	结合应用协议识别功能，可以根据用户的应用协议类别进行流量管理。
基于 IP 的流控	根据源 IP 地址/地址组进行流量管理。
基于用户组的流控	可以为不同用户组采取不同的流量管理措施。
基于时间段的流控	可以根据不同的时间段，进行差异化的流量管理。
基于单个用户的流控	可根据主机的 IP 地址或者用户名称，对单个主机进行如下控制： 最大上行/下行带宽限制； 最大上行/下行会话控制； 分类服务的带宽控制，即限制单主机的总带宽的同时，再对某些服务进行控制。如限制单个主机的上行/下行带宽分别为 500K/1M 的同时，再限制 P2P 的带宽为 100K/200K、网络电视为 100K/100K 等；

	以上参数均可分时段管理。
黑名单管理	
共享上网	针对通过无线路由器、360WiFi 等共享上网的行为进行检测，单 IP 超过设定终端数，该 IP 将进入防共享上网列表。
流量配额	可根据每日、每周、每月的流量配额来控制用户，当用户的流量超过预设配额时，将用户进入黑名单。
速率控制	当用户连续一段时间(如 5 分钟)内的上行或下行流量持续超过预设阀值，将用户进入黑名单。
并发会话数控制	当用户连续一段时间(如 5 分钟)内的上行或下行并发会话数持续超过预设阀值，将用户进入黑名单。
新增会话数控制	当用户连续一段时间（如 5 分钟）内的上行或下行新增会话数持续超过设定阈值，将进入黑名单。
基于时间段控制	在某些时间段（如下班时间，凌晨），不对用户的速率和会话数进行限制，用户产生的流量也不记入黑名单的流量配额内。
多种惩罚方式	当用户进入黑名单后，可以将用户强制下线，也可以修改用户的上行速率、下行速率、上行会话、下行会话等。
加倍惩罚	在一周内、一月内、一季度内，连续进入黑名的次数超过预设次数，惩罚时间可以加长为原来的几倍。
终端类型	可针对移动终端、PC 及其他终端类型设定控制策略。
白名单管理	
基于内网用户	可对内网用户（IP 地址、地址范围、地址簿、用户组）进行白名单的控制。

的白名单	
基于外网 IP 地址白名单	可对内网用户访问特定的互联网 IP 地址（IP 地址、地址范围、地址簿）进行白名单的控制。
基于时间段的控制	可根据时间段进行白名单的控制。
流量实时监控	
TOP 50 服务流量监控	查看前五十名服务流量的实时监控。
服务组流量监控	将各服务分类统计，实时查看服务组流量监控图。
活跃服务统计	查看当前活跃服务的最新速率、最近一小时流量、最近一小时平均速率、每个服务对应有哪些用户在使用，及每个用户的使用情况。
所有服务统计	查看当前活跃服务的最新速率、最近一小时流量、最近一小时平均速率。
TOP 50 用户流量监控	查看前五十名用户的传输速率、新建会话速率、活跃会话数。
在线用户统计	实时查看当前在用户的详细信息：在线流量、最新速率、会话数、上线时间等信息。
上网行为	实时查看在线用户的访问网站、搜索引擎、邮件收发、账号登录等上网行为记录。
物理端口	查看物理端口接收报文的情况，以及每个端口传输流量的趋势图。
动态更新实时	支持动态显示网络流量监控图。

监控图	
防共享上网	通过无线路由器、360WiFi 等共享上网行为的惩罚列表。
当前黑名单	超出黑名单策略阈值进入黑名单的惩罚列表。
上网审计管理	
审计策略	默认全部审计，可设定规则实现部分部分用户审计，部分上网行为审计。
审计选项	可指定审计方式、审计的文件大小上限、会话审计方式、访问网站日志记录选项。
终端类型	可指定移动终端、PC 及其他终端的上网行为的审计规则。
用户管理	
组织结构	可建立与企业组织结构相同的网络组织结构，将用户划分到对应用户组中。每个用户或用户组都可以有自己的上网策略及权限。
临时账户管理	支持临时用户自主申请临时账户，主要提供给外来的临时用户使用。支持自动审核和管理员手动审核的核定方法将临时账户加入到组织结构中。减少管理员对临时账户的频繁配置，统一临时账户的上网权限和使用期限的管理。
批量生产临时帐号	支持批量生产临时帐号，可指定生产个数和有效时间。并通过邮件收取临时账户密码功能。
本地认证	将用户信息存储于设备内，认证时无须第三方服务器。
AD 域认证	支持 AD 域认证，便于与组织内部原有域认证融合。
RADIUS 认证	支持与第三方 RADIUS 服务器联动认证。
LDAP 认证	支持 LDAP 认证，便于与组织内部原有 LDAP 认证融合。

POP3 认证	支持与现存的 POP3 服务器中的账户信息进行联动认证，简化配置、方便部署。
WEB 认证	结合本地数据库、POP3、AD、LDAP 或 RADIUS 服务器等认证方式，为接入用户提供 Web 认证功能。
短信认证	支持通过短信验证码、密码/短信认证组合的认证方式。（外接 USB 短信猫或第三方短信网关联动认证）
LDAP/AD 导入	可按照 LDAP/AD 等服务器组织架构导入用户/用户组信息。
用户同步	可将 LDAP、AD 等外部服务器的用户信息同步到设备中，无须在手动添加用户信息。
用户导入	可将已导出的用户信息的文件，或根据规定的用户格式编辑文件，批量导入用户信息。
自动创建账户	对于未创建的账户，可根据其 IP 地址、MAC 地址、主机名或者 VLAN ID 等作为新用户名自动创建账户，并可同时绑定 IP、绑定 MAC、绑定 IP+MAC、绑定 VLAN，并自动分配到指定用户组，享有指定网络权限。
终端识别	支持终端类型（PC，android，苹果）识别，可识别操作系统类型及对应 IP 地址。
IP/MAC 绑定	支持绑定 IP、绑定 MAC、绑定 IP+MAC。
VLAN 绑定	支持 VLAN 绑定。
免认证功能	可设定特殊 IP 不需要认证即可访问网络。
认证通过后显	可将认证通过的用户强制导向到企业入口网页，如组织的公告页面等。

示指定页面	
自定义认证页面	支持自定义的用户认证登录页面。
认证冲突处理	支持账户重复登入 ,当超出最大登入允许数后 ,支持是否踢掉前一次登入。
内网主机扫描	可通过 NetBIOS 协议扫描内网的主机信息 ,扫描结果将列出每个主机的 IP 地址、MAC 地址和主机名等，然后可以将其加入某个用户组中，逐步完善组织结构的管理。
自身安全防护	
高可靠性(HA)	支持一主一备模式的 HA 功能。
防 DOS 攻击	防止设备自身遭受 DOS 攻击。
防 ARP 欺骗	定期发送 ARP 广播，防止网关设备 ARP 被篡改。
会话加速老化	对某些会话进行快速老化，防止会话表被写满。
告警配置	
设备告警	支持设备事件日志告警、黑名单告警、CPU、内存、活跃会话数等告警。
非法网站告警	支持对自定义非法网站访问的告警设置。
故障排除	
调试信息下载	一键下载故障信息，以便研发人员分析故障。
报表中心	
内置报表中心	设备内置报表中心系统，实现上网行为记录与日志的存储、查询、审计，以及报表的生成等。
外置报表中心	将报表数据自动转存于外置独立服务器，以数据库形式存储。可避免设备

	内置存储空间有限和对性能的影响。
图形化日志统计工具	通过图形化的报表中心，方便用户对行为记录的查询、审计、统计，并支持以饼状图、柱状图、曲线图等形式直观显示统计结果。
分层管理	根据管理员的权限，可以查看到只属于其管辖范围的用户的统计资料。
报表生成	可将报表中心相关内容转换为 Excel、PDF 报表，大大简化了管理员手工制作报表。
自动邮件告警	对特定安全事件支持通过邮件自动告警
自动短信告警	对特定安全事件支持通过短信自动告警
统计分析	
设备资源	分时段对设备资源，包括 CPU 使用率、内存使用率、活跃会话数、在线用户数等信息进行统计分析。
物理接口	分时段对物理接口的收发的流量、速率等进行统计分析。
用户统计	基于用户，对其流量、新建会话、活跃会话进行分时段统计分析，并进一步统计分析每个用户使用了哪些服务、访问了哪些网站、通过了哪些链路等更加详细的信息。
用户组统计	基于用户组，对其流量、新建会话、活跃会话进行分时段统计分析，并进一步统计分析每个用户组使用了哪些服务、访问了哪些网站、通过了哪些链路等更加详细的信息。
服务统计	基于服务名称，对其流量、新建会话、活跃会话进行分时段统计分析，并进一步统计分析每种服务有哪些用户/用户组在使用，及每个用户/用户组的使用情况；以及每种服务在各条链路上的分配情况。

服务类型统计	基于服务类型，对其流量、新建会话、活跃会话进行分时段统计分析，并进一步统计分析每种类型的服务有哪些用户/用户组在使用，及每个用户/用户组的使用情况；以及每种服务类型在各条链路上的分配情况。
网站统计	基于 URL，对其流量、新建会话、活跃会话进行分时段统计分析，并进一步统计分析每个 URL 的服务有哪些用户/用户组在使用，及每个用户/用户组的使用情况；以及每种服务类型在各条链路上的分配情况。
网站类型统计	基于网站类型，对其流量、新建会话、活跃会话进行分时段统计分析，并进一步统计分析每种类型的网站有哪些用户/用户组在使用，及每个用户/用户组的使用情况；以及每种服务类型在各条链路上的分配情况。
线路统计	基于出口链路，对其流量、新建会话、活跃会话进行分时段统计分析，并进一步统计分析每条链路上的用户、用户组、服务、服务类型、网站、网站类型的详细信息。
网站访问量排名	基于用户/用户组对 URL 的访问次数，进行统计排名。 基于网站/网站类型被访问的次数，进行统计排名。
网页文件下载排名	基于用户/用户组，通过网页下载的文件次数，进行统计排名。 基于文件类型被下载的次数，进行统计排名。
上网时长统计	统计用户上网的总时长，并统计每类服务使用时间的情况。
日志查询	
DoS 攻击日志	记录 DoS 攻击日志，包括攻击类型、源区域、源目 IP 地址、目的 IP 地址、匹配策略名、描述、严重级别、记录时间。
IPS 日志	记录 IPS 日志，包括攻击类型、源区域、源目 IP 地址、目的端口、漏洞

	ID、漏洞名称、匹配策略名、描述、严重级别、记录时间。
病毒查杀	记录病毒查杀日志，包括应用类型、行为、协议、文件名、文件类型、病毒名称、源目区域、源目 IP、源目端口、所属组、记录时间。
网页 URL 日志	能够记录用户所访问网站的 URL 地址。
会话记录	详细记录每一个会话的信息，包括：用户名、用户组、源 IP/端口、目的 IP/端口、转换 IP/端口、MAC 地址、协议类型、协议名称、发送流量、接收流量、会话持续时间、会话结束时间。并可导出为 EXCEL 或者 HTML 格式的报表。
告警记录	记录非法网站的告警日志。
高级检索	可查询以上日志类型，支持模糊查询。
数据管理	
数据存储策略	支持按磁盘百分比、按保留天数、系统硬盘最大化三种存储方式。
数据列表查询	支持查询磁盘空间使用和剩余空间、百分比，包括每一种数据类型的使用空间、磁盘占用率，时间范围。
数据删除	基于时间范围、数据类型明细、系统日志明细删除日志。
数据备份	支持备份本地存储日志到 FTP 服务器，为日志审计提供冗余备份。